UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/817,670	03/26/2001	Eric Hughes	EH-2001-01	8660

7590 08/25/2004

Eric Hughes
1577 Rose Street
Berkeley, CA 94703

EXAMINER	
NALVEN, ANDREW L	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 08/25/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/817,670	HUGHES, ERIC	
	Examiner	Art Unit	
	Andrew L Nalven	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 March 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *26 March 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-20 are pending.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-2, 4-7, 9-14, and 16-19 are rejected under 35 U.S.C. 102(b) as being anticipated by Kocher US Patent No. 5,903,651. Kocher discloses a method for demonstrating and confirming the status of digital certificates and other data.

4. With regards to claim 1, Kocher teaches the arranging of a plurality of messages into an ordered sequence of messages (Kocher, column 6 lines 43-47 "data items...sorted in ascending order", column 11 lines 33-50), constructing a hash tree from the sequence of messages (Kocher, column 7 lines 19-26, hash tree), computing a value of a root node of a hash tree (Kocher, column 7 lines 51-54, root node), preparing a private key for a digital signature operation (Kocher, column 1 lines 46-50), and performing a cryptographic signature operation with the private key upon the value of the root node (Kocher, column 8 lines 5-13).

5. With regards to claims 2 and 13, Kocher teaches the tree constructed with a position dependent hash function (Kocher, column 7 lines 40-43, hash depends on level in the tree).

6. With regards to claim 4, Kocher teaches a value of the leaves of the hash tree being taken as the results of a hash function applied to the values of the sequence of messages (Kocher, column 7 lines 33-44, cryptographic hash function).

7. With regards to claims 5, 9, 11 and 18, Kocher teaches the performing of the cryptographic signature operation with padding added to the value of the root node (Kocher, column 8 lines 5-13, padding viewed as date/time stamp, number of nodes, see Figure 9 item 905).

8. With regards to claim 6, Kocher teaches all that is described above, and further teaches the extracting of the public key digital signature from a combination of the hash tree and from the results of the cryptographic signature operation (Kocher, column 9 lines 26-42).

9. With regards to claims 7 and 19, Kocher teaches the incorporating of a hash tree size into the public key digital signature where the hash tree size is the number of the plurality of messages (Kocher, column 8 lines 5-13 "number of nodes", see Figure 9 item 904).

10. With regards to claims 10, 12 and 17, Kocher teaches the parsing of the public key digital signature and the retrieving of its signature data (Kocher, column 8 lines 34-38, column 9 lines 26-36), the ascertaining that the signature data comprises a stated signature value and a stated sibling value and position sequence (Kocher, column 8

lines 29-32), computing a hash tree branch comprising a leaf node and a root node (Kocher, column 10 lines 1-20, column 9 lines 39-44, Figure 14), the hash tree branch being computed with the value of the individual message and with the stated sibling value and position sequence (Kocher, column 9 lines 39-44), and performing a verification operation on the stated signature value with the value of the root node and with the public key (Kocher, column 9 liens 26-52).

11. With regards to claim 14, Kocher teaches the ascertaining that the signature data comprises a hash tree size (Kocher, column 9 lines 60-61), the determining of a tree representative of the tree family and whether or not the shape of the hash tree branch is a valid branch of the tree (Kocher, column 9 line 53 – column 10 line 20).

12. With regards to claim 16, Kocher teaches the value of the leaf of the hash tree branch taken as the result of a hash function applied to the value of the individual message (Kocher, column 7 lines 33-43).

Claim Rejections - 35 USC § 103

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

14. Claims 3, 8, 15, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher US Patent No. 5,903,651 in view of Ostrovosky et al US Patent No. 5,123,045.

15. With regards to claims 3, 8, 15, and 20, Kocher fails to teach the hash tree constructed using a hash function with a salt value. Ostrovosky teaches a hash tree constructed using a hash function with a salt value (Ostrovosky, column 6 lines 46-67). At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to utilize Ostrovosky's method of hashing with Kocher's system because it offers the advantage of providing a random function that helps prevent attackers from corrupting memory locations (Ostrovosky, column 3 lines 28-57).

Conclusion

16. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

17. Simon et al US Patent No. 6,065,008 discloses a system for secure font subset distribution.

18. Kaliski Jr US Patent No. 6,189,098 discloses a client/server protocol for proving authenticity.

19. Ansper et al US PG Pub 2001/0032314 discloses a method for validating a digital signature.

20. Karjoth et al US PG Pub 2001/0034839 discloses a method for secure transmission of data and applications.

21. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L Nalven whose telephone number is 703 305 8407. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 703 308 4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalven

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100